

FIG.1

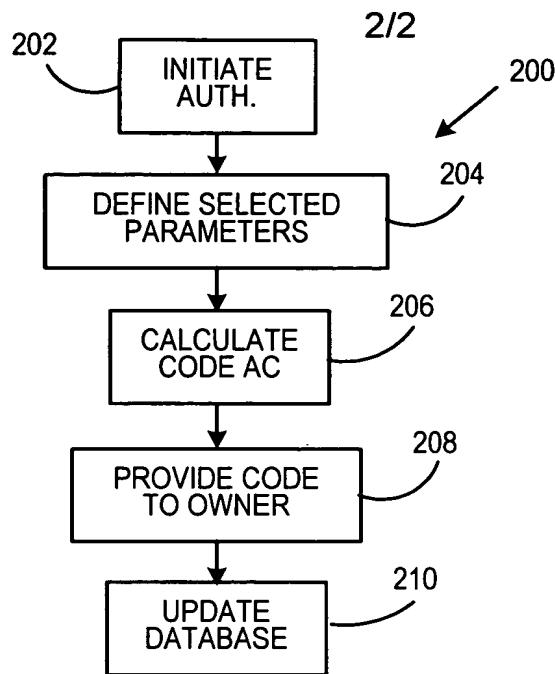


FIG. 2

$$AC = DES \{ PD_1, PD_2, \dots, PD_N; K \} = CAC$$

FIG. 2A

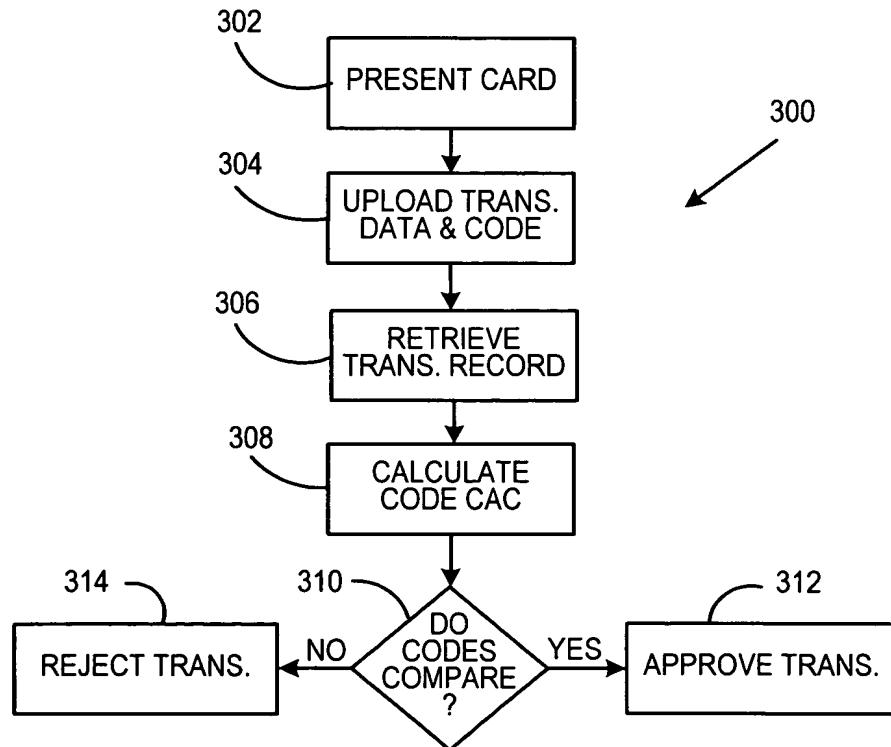


FIG. 3